IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): He	
Application No.: 10/661903	Group Art Unit: 2131
Filed: 9/12/2003	Examiner: Chai
Title: Scalable Distributed Method and Apparatus for Transforming Packets to Enable Secure Communication Between Two Stations	
Attorney Docket No.: 120-161	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Please enter this Appeal Brief. A Notice of Appeal was filed on September 8, 2008.

I. Real Party in Interest

The real party in interest is Nortel Networks Limited.

II. Related Appeals and Interferences

Appellants are not aware of any related appeals or interferences.

III. Status of the Claims

Claims 1, 6-9 and 11 are pending in this application. All of the pending claims are rejected. Claims 1, 9 and 11 are previously presented. Claims 6, 7 and 8 are original. Claims 2-5, 10 and 12-15 were cancelled. The rejections of independent claims 1, 9 and 11 are the subject of this appeal.

IV. Status of Amendments

All submitted amendments have been entered and considered.

V. Summary of Claimed Subject Matter

The invention helps to provide secure communications in a network environment. VPNs and IPsec tunneling involve point-to-point connections between sites. This creates a scalability problem because the amount of data stored to support N connections in the network grows at the rate of N^2 -1. In a network having a thousand endpoints, data may need to be stored identifying paths and authentication for the million connections between the endpoints. Various proposals have been made to overcome the scalability issues associated with VPNs, but each have drawbacks. For example, at least one proposed solution requires that a high level of trust be placed on the Service Provider to protect Customer data. Encrypted tunneling can be used to lower the need for such trust. However, overlaying traditional encrypted tunneling methods on top of the IP VPN structure simply introduces more point-to-point security associations, thereby eliminating the scalability benefits of the IP VPN architecture. The presently claimed invention helps to overcome these drawbacks by utilizing a group security association instead of multiple point-to-point security associations, i.e., the same group security association for different connections.

Support for the limitations recited in the claims is in the specification as indicted below.

1. (previously presented) A method of securing packet data transferred between a first and second member of a private network coupled to client edge devices over a backbone comprising a plurality of provider devices including provider edge devices, the backbone operating according to a routing protocol, the method comprising the steps of:

encapsulating a private address of a packet from the first member with a group header including a public address associated with the first member and a group address to generate a tunneled packet; **"When a member of the private network seeks to communicate with another member, it simply forwards the communication to the trusted ingress point 6 with a Virtual Private Network (VPN) group address associated with the other member." Page 9, lines 19-21**

transforming, at a client edge device, the tunneled packet by first applying a group security association associated with the private network to the tunneled packet to provide a secure tunneled packet and then adding a header field to the secure tunneled packet, the added header field including a gateway address associated with the first member of the private network and a destination address of the second member of the private network to provide a client transformed packet; **"The trusted ingress point uses the security association associated with the private network to transform the communication." Page 9, lines 21-23; "At step 200, the CE (which is also referred to as the IPsec gateway) encapsulates the IP header data with the Group IP header defined in the IP VPN protocol. That is, as shown in Figure 9A, a group header, with a source equal to the IP Gateway address, the Destination equal to the VPN ID, and Next Header Type field indicating an IP VPN type header is pre-pended to the IP header 140." Page 19, lines 3-8.**

forwarding the client transformed packet to a provider edge device; **"The trusted ingress point ... forwards the transformed communication through other intermediate stations in the network (such as station 7), until it reaches the trusted egress point 8." Page 9, lines 21-25** and

replacing, at the provider edge device, a destination field of the packet with a group identifier associated with the private network for routing the packet across the backbone **"The trusted egress point uses the stored security association corresponding to the Virtual Private Network (VPN) group address to decode the transformed communication and forwards the communication to the appropriate destination." Page 9, lines 25-27.**

9. (previously presented) A method of securing packet data transferred between a first and second member of a private network over a backbone, the first and second member of the private network being coupled to respective client edge devices and the backbone comprising a plurality of provider devices including provider edge devices, the backbone operating according to a routing protocol, the method comprising the steps of:

determining, responsive to a gateway address of a packet, whether a packet received from a client edge device at a provider edge device of the backbone has been transformed to secure packet data transferred across the backbone; **"Referring now to Figure 10A, at step 210, when the PE receives**

the packet 180, it performs the VRF lookup using the value in the Destination Field 157 to find the routing data necessary to forward the packet (for example, an MPLS label). At step 212, the value in the Source field is evaluated to determine whether it is the IPsec Gateway Address. If it is the IPsec Gateway address, it signals the PE that the CE had previously transformed the packet data." Page 19, lines 14-19

modifying at least one field of the packet to replace a destination address of the packet with a group identifier associated with the private network responsive to a determination that the gateway address of the packet indicates that the packet is a member of the private network. **"As a result, if it is the gateway address, the PE replaces the value in the Destination Address field with the VPN-ID, which is available from the VRF. The packet can then be transferred directly to the CE." Page 19, lines 19-21**

11. (previously presented) A system for transforming packets for forwarding between a plurality of members coupled to client edge devices of a private network over a backbone comprised of a plurality of provider devices including provider edge devices in a scalable private network, wherein the backbone operates according to a protocol, the apparatus comprising:

a key table, the key table including a security association for each private network that the node is a member; **"The GCKS 30 is shown to include various representative components, including a key table 32." Page 12, lines 10-11; "The key table 32 includes a number of entries, such as entry 33, which stores a key for each group ID." Page 12, lines 14-16**

a client edge device including:

a tunneling mechanism for encapsulating packets that are to be transferred to the backbone in a public address including a gateway address and a group address to provide a tunneled packet; **"At step 200, the CE (which is also referred to as the IPsec gateway) encapsulates the IP header data with the Group IP header defined in the IP VPN protocol. That is, as shown in Figure**

9A, a group header, with a source equal to the IP Gateway address, the Destination equal to the VPN ID, and Next Header Type field indicating an IP VPN type header is pre-pended to the IP header 140. The value in the Destination Field 146 of the original IP header is saved. Page 19, lines 3-9

and

transform logic operable to apply a security association to the tunneled packet and to append a header to the tunneled packet, the header including a gateway address and a destination address to provide a transformed packet for transmission by the client edge device to the backbone; **"At step 202, normal IPsec processing is performed on the outer IP header (i.e., the gateway IP, Group IP address) to provide the CE transformed packet 180. Note that in this implementation, the entire original packet (including header 140 and payload) may be encrypted and authenticated. The previously saved value from the Destination field 146 is used to overwrite the Group IP address. The CE transformed packet is then transferred to the PE." Page 19, lines 10-15**

a provider edge device coupled to the client edge device, the provider edge device comprising a virtual route forwarding table for storing group identifiers associated with destination addresses and means, responsive to the gateway address of the header, for selectively updating the destination field of the packet with a group identifier for routing the packet across the backbone. **"Referring now to Figure 10A, at step 210, when the PE receives the packet 180, it performs the VRF lookup using the value in the Destination Field 157 to find the routing data necessary to forward the packet (for example, an MPLS label). At step 212, the value in the Source field is evaluated to determine whether it is the IPsec Gateway Address. If it is the IPsec Gateway address, it signals the PE that the CE had previously transformed the packet data. As a result, if it is the gateway address, the PE replaces the value in the Destination Address field with the VPN-ID, which is available from the VRF. The packet can then be transferred directly to the CE. Standard packet**

processing techniques are performed in the CE in this embodiment." Page 19, lines 16-24

VI. Grounds of Rejection to be Reviewed on Appeal

Claims 1, 9 and 11 are rejected under 35 U.S.C. 103(a) based on US 2002/0154635 (Liu) in combination with US 6,970,941 (Caronni) and US 6,185,650 (Shimbo)

VII. Argument

A. The presently claimed invention is distinct because it utilizes the same group security association for different connections.

The invention helps to provide secure communications in a networked environment. VPNs and IPsec tunneling involve point-to-point connections between sites. This creates a scalability problem because the amount of data stored to support N connections in the network grows at the rate of N^2 -1. In a network having a thousand endpoints, data may need to be stored identifying paths and authentication for the million connections between the endpoints. Various proposals have been made to overcome the scalability issues associated with VPNs, but all have drawbacks. For example, at least one proposed solution requires that a high level of trust be placed on the Service Provider to protect the Customer data. Encrypted tunneling can be used to lower the need for such trust. However, overlaying traditional encrypted tunneling methods on top of the IP

VPN structure simply introduces more point-to-point security associations, thereby eliminating the scalability benefits of the IP VPN architecture. The presently claimed invention helps to overcome these drawbacks by utilizing a group security association instead of multiple point-to-point security associations, i.e., the same group security association for different connections.

In response to the arguments previously submitted by applicant, the examiner asserts that Caronni teaches providing security at column 2, lines 27-33, column 4, lines 38-52, column 12.lines 50-52, and figure 6/2B. The examiner further asserts that Caronni teaches application of security to a group of addresses at column 3, lines 22-26, column 4, lines 58-60, and column 7, lines 5-33. Applicant basically agrees with the examiner. However, these well known features are already discussed in the background of this application and merely represent the problem, not the claimed solution.

Point-to-point security associations are well known. Group security associations are well known. What is novel is the application of the same group security association to non-group point-to-point communications. The examiner appears to interpret "group security" as meaning security applied to any group of devices. However, as understood in the art, "group security" is security applied to a group of devices that share the same connection, e.g., multicast. Since the devices share the same connection, there is no concern about different members of the group sharing the same security association. However, this lack of concern does not hold true for members of a group that do not share the same connection, i.e., members exchanging different (non-group) communications. Consequently, each non-group connection has traditionally been assigned a unique point-to-point security association. The presently claimed invention is distinct because it utilizes a group security association instead of multiple point-to-point security associations, i.e., the same group security association for different connections. The problem of maintaining security between different members of the "group" is solved by applying the group security association at edge devices that are commonly trusted by all members.

The problem with applying point-to-point security associations to a group of devices, e.g., as in Caronni, is explained in the Background at page 2, lines 19-24. Because each secure connection requires storage of security association data, the amount of data that must be stored to support N point-to-point connections increases at a rate of N^2-1. This rate of increase causes a scalability problem because the amount of data that must be stored and searched becomes very large. The scalability problem is at least mitigated by utilizing a group security association for different connections between members of a private network, e.g., store one group security association from the entire private network rather than individual security associations for each point-to-point or member-to-member connection. As discussed above, this solution is counter-intuitive because members not sharing a connection could technically obtain access to each other's data. However, the possibility of such an occurrence is reduced by applying the group security association at trusted edge devices.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d

981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). With regard to the limitation of "transforming, at a client edge device, the tunneled packet by first applying a group security association associated with the private network to the tunneled packet to provide a secure tunneled packet and then adding a header field to the secure tunneled packet, the added header field including a gateway address associated with the first member of the private network and a destination address of the second member of the private network to provide a client transformed packet," as recited in claim 1, and the corresponding limitations recited in claims 9 and 11, the Examiner cites Caronni at column 2, lines 22-33, column 4, lines 38-52 and 58-60, column 7, lines 5-33, column 12, lines 50-52, and figure 6/2B. The flaw in the rejection is that the cited passages merely describe application of security to a group of devices. In particular, Caronni would apply a unique point-to-point security association to each member of the group, thereby incurring the scalability problem discussed above. The point that seems to elude the Office is that application of security to a group of devices is not equivalent to application of a *group security association* to different point-to-point connections between members of the group. Applicant has studied Caronni and the other references and finds *no suggestion that the same group security association can be applied to different connections*. Because Caronni fails to describe applying a group security association associated with the private network to the tunneled packet to provide a secure tunneled packet, claims 1, 9 and 11 distinguish the cited combination.[1]

VIII. Conclusion

The rejections are improper for at least the reasons set forth above. Appellants accordingly request that the rejections be withdrawn and the application put forward for allowance.

Respectfully submitted,

/Holmes W. Anderson/
Holmes W. Anderson
Reg. No. 37,272
Attorney for Assignee

Date: October 7, 2008

Anderson Gorecki & Manaras LLP
33 Nagog Park
Acton MA 01720
(978) 264-4001

[1] Note that Liu and Shimbo are not cited as showing this novel feature and are therefore not discussed in detail. However, Applicant does not concede the asserted characterizations of those references.

Appendix A - Claims

1. (previously presented) A method of securing packet data transferred between a first and second member of a private network coupled to client edge devices over a backbone comprising a plurality of provider devices including provider edge devices, the backbone operating according to a routing protocol, the method comprising the steps of:

encapsulating a private address of a packet from the first member with a group header including a public address associated with the first member and a group address to generate a tunneled packet;

transforming, at a client edge device, the tunneled packet by first applying a group security association associated with the private network to the tunneled packet to provide a secure tunneled packet and then adding a header field to the secure tunneled packet, the added header field including a gateway address associated with the first member of the private network and a destination address of the second member of the private network to provide a client transformed packet;

forwarding the client transformed packet to a provider edge device; and

replacing, at the provider edge device, a destination field of the packet with a group identifier associated with the private network for routing the packet across the backbone .

2. (cancelled)
3. (cancelled)
4. (cancelled)
5. (cancelled).

6. (original) The method according to claim 1, wherein the group security association is associated with each member of the private network.

7. (original) The method according to claim 1, further comprising the steps of:

each member of the private network registering with a global security server;

the global security server forwarding the group security association to each member of the private network.

8. (original) The method according to claim 7 including the step of the global security server periodically forwarding a new group security association to each member of the private network.

9. (previously presented) A method of securing packet data transferred between a first and second member of a private network over a backbone, the first and second member of the private network being coupled to respective client edge devices and the backbone comprising a plurality of provider devices including provider edge devices, the backbone operating according to a routing protocol, the method comprising the steps of:

determining, responsive to a gateway address of a packet, whether a packet received from a client edge device at a provider edge device of the backbone has been transformed to secure packet data transferred across the backbone;

modifying at least one field of the packet to replace a destination address of the packet with a group identifier associated with the private network responsive to a determination that the gateway address of the packet indicates that the packet is a member of the private network.

10. (cancelled)

11. (previously presented) A system for transforming packets for forwarding between a plurality of members coupled to client edge devices of a private network over a backbone comprised of a plurality of provider devices including provider edge devices in a scalable private network, wherein the backbone operates according to a protocol, the apparatus comprising:

a key table, the key table including a security association for each private network that the node is a member;

a client edge device including:

a tunneling mechanism for encapsulating packets that are to be transferred to the backbone in a public address including a gateway address and a group address to provide a tunneled packet; and

transform logic operable to apply a security association to the tunneled packet and to append a header to the tunneled packet, the header including a gateway address and a destination address to provide a transformed packet for transmission by the client edge device to the backbone;

a provider edge device coupled to the client edge device, the provider edge device comprising a virtual route forwarding table for storing group identifiers associated with destination addresses and means, responsive to the gateway address of the header, for selectively updating the destination field of the packet with a group identifier for routing the packet across the backbone.

12. (cancelled)

13. (cancelled)

14. (cancelled)

15. (cancelled)

Appendix B - Evidence Submitted

None.

Appendix C - Related Proceedings

None.